STATEMENT

OF

GEORGE FORESMAN

UNDERSECRETARY FOR PREPAREDNESS
U.S. DEPARTMENT OF HOMELAND SECURITY

BEFORE THE

SUBCOMMITTEE ON ECONOMIC SECURITY,
INFRASTRUCTURE PROTECTION AND CYBER
SECURITY

COMMITTEE ON HOMELAND SECURITY
UNITED STATES HOUSE OF REPRESENTATIVES

September 13, 2006

Good morning, Mr. Chairman and Members of the Subcommittee. Thank you for inviting me to speak about cyber security and the recovery and reconstitution of critical networks in the event of a catastrophic Internet disruption.

One of the most pressing challenges facing the Department of Homeland Security is preparing for attacks on the Internet and the information networks supporting our critical infrastructure. Our vision, our philosophy, and our strategy for preventing, responding to, and recovering from cyber attacks reflect the expanding importance of communications and the information infrastructure in all aspects of our lives today. Policies that advance a safe and secure communications infrastructure rely on fostering valuable relationships between the public and private sectors, and promoting public trust and confidence. Strong policies also project stability and strength to those who wish us harm.

The key to continued success is partnering strategically with the communications and information technology sectors, end-users of Internet technologies, and other experts.

During the past several weeks our cyber security experts worked quietly with their counterparts at Microsoft to address a critical software vulnerability first identified to us by the Department of State's cyber defense team. In the interim between identification of the vulnerability and development of the solution, the Department was closely monitoring technical indicators for indications of additional exploitation of the vulnerability. Once a patch was available, the Department's U.S. Computer Emergency Readiness Team (US-CERT) coordinated an alert with Microsoft. DHS issued an alert through the National Cyber Alert System urging the public, private industry, as well as federal users to apply the security patch in order to protect their systems. Overshadowed in the news media by the successful foiling of the U.K. terror threat, this collaboration is typical of the kind of behind-the-scenes, day-to-day public-private cyber security activity that exemplifies the work being accomplished between the Department and so many of our strategic partners.

These partnerships also entail strengthening cooperation across the government institutions and, at a minimum, finding ways to cultivate support outside of the Department where expertise clearly exists. We are actively collaborating with 116 private firms. We are working closely with the private sector entities established within the National Infrastructure Protection Plan (NIPP) framework to collaborate on risk management, including the Information Technology (IT) Sector Coordinating Council (SCC) and the Telecommunications SCC. From an operational

perspective, we work with the Information Technology Information Sharing and Analysis Center (IT-ISAC) and the National Coordinating Center (NCC)/Telecommunications ISAC through various information sharing mechanisms, including the US-CERT Portal. Our partners, both public and private, are involved in a number of programmatic activities that address software assurance, Internet disruption, as well as exercises such as Cyber Storm.

In addition, there are about 400 firms that are part of the Process Control Systems Forum, which was recently transferred from Science and Technology Directorate to National Cyber Security Division (NCSD) and addresses Control Systems security. There are 21 associations that we work with on a regular basis that represent hundreds of companies, including large enterprises and smaller companies. Whether public or private, these partnerships must deliver real and measurable value in light of the catastrophic damages that could occur to our national cyber assets if we do not collaborate effectively.

Finally, we must reinforce a culture of preparedness and increasingly shift from a reactive to a proactive stance. In sum, we must prepare by promoting effective security strategies that evolve as the risks evolve.

Assistant Secretary for Cyber Security and Telecommunications

Mr. Chairman, the Committee has expressed as a priority the designation of the Assistant Secretary for Cyber Security and Telecommunications, and has communicated interest in the Department's plan to fill this vacancy.

Mr. Chairman, the Department shares the Committee's view on the importance of filling the position of Assistant Secretary for Cyber Security and Telecommunications with a qualified candidate.

Given the complexity of the portfolio, we believe it is important to fill this position with a person of necessary talent and expertise who understands both policy and technology issues regarding cyber security and telecommunications and can further strengthen our national efforts. I am personally engaged in this process and, in the interim, am providing program direction to the talented men and women who are part of our NCSD and National Communications System (NCS). Because of the importance of our mission, all parties want to ensure that the individual appointed to this position possesses the right combination of skills, experience, and leadership necessary to succeed.

In the interim, I want to assure you, Mr. Chairman, that I am personally overseeing strategic management objectives associated with NCSD and specifically Internet recovery. These include, by way of example:

- Positioning the NCSD, especially the US Computer Emergency Readiness Team (US-CERT), and the NCS so these organizations are structured to be at the forefront of preventing, responding to, and recovering from massive Internet disruptions. Just as FEMA is on point for coordinating disaster response, and the Coast Guard is on point for coordinating the response to an oil spill, key experts like NCS and NCSD must be capable of coordinating our response to events that target the Internet;

- Re-aligning CS&T component entities to create a cohesive organization. The NCS and NCSD (including the US-CERT and the NCC) must more fully synchronize their activities, without a loss of either's core mission capabilities. Communications convergence, threats against the communications infrastructure, the increasing use of Voice over Internet Protocol (VOIP) for emergency communications purposes, and other influences demand that we merge the work of these entities to create new and stronger synergies and;

- Ensuring resources are sufficiently allocated to meet new needs. I am personally overseeing the development of a budget strategy that spans the next five years. This strategy is essential for shepherding CS&T priority programs into the next decade.

Information Sharing and Internet Recovery
Mr. Chairman, the Committee has communicated interest in the programs within the Department that are designed to improve information sharing regarding the recovery of the Internet

We fully recognize the challenges inherent in our preparedness responsibilities. As the President stated in the *National Strategy to Secure Cyberspace*, it is the policy of the United States to protect against "the debilitating disruption of the operation of information systems for critical infrastructures and, thereby, help to protect the people, economy, and national security of the United States." The strategy also underscores the importance of partnering with the private sector as well as State, local, and tribal governments to effectuate this policy.

On my fourth day as Undersecretary for Preparedness, I met with the Business Roundtable to discuss strategic collaboration and their Internet

reconstitution study. We outlined a 120-day plan to advance our collaboration on this important work and continue to work in tandem with the Roundtable as they expand their efforts to focus on business needs and issues regarding Internet recovery and reconstitution in the coming year. The timeframes for specific actions and results will be the topic of more discussion with the Business Roundtable in the next several months. That effort supplements the work we are doing with the IT-SCC and the Telecommunications SCC under the NIPP to address Internet protection and prioritization as part of our collaborative approach to risk management in the core sectors for the Internet.

US-CERT, NCC & the NAIRG

In addition to coordinating with the Business Roundtable, our outreach specifically focuses on building relationships with private industry owners and operators of the Internet and information networks. For example, the US-Computer Emergency Readiness Team (US-CERT) continues to develop operational relationships and processes to enhance its ability to respond to an Internet disruption of national significance through its work with the IT-ISAC, and with the North American Incident Response Group (NAIRG) of industry participants. In addition, the NCC represents a fully collaborative model as the ISAC for the Telecommunications Sector, with both public and private participation in its operations.

The US-CERT has deployed several programs as part of its efforts to support cyber incident response. We expect funding in Fiscal Year 2007 to reach approximately $37 million. These funds support deployment of multiple programs, including the Einstein Program, which tracks attacks on federal information systems and warns stakeholders in near real-time. Other program areas funded as part of this total include an Internet Health Service for federal agency incident response teams, the US-CERT's 24X7 cyber incident handling center, vulnerability management, forensics education and support, and malicious code analysis.

Internet Disruption Working Group (IDWG)

The NCSD and NCS have also established an Internet Disruption Working Group (IDWG) to address the resiliency and recovery of Internet functions in the event of a major cyber incident. With public and private sector representatives, the IDWG's near-term objectives help to augment the level of information sharing among government and the private sector. The IDWG is also undertaking an information sharing assessment

to better understand the information exchange landscape involving Internet incidents.

National Cyber Response Coordination Group (NCRCG)

The Business Roundtable report also underscores the role of the National Cyber Response Coordination Group (NCRCG). Established in partnership with the Department of Defense and the Department of Justice in the National Response Plan's (NRP) Cyber Annex, the NCRCG serves as the Federal government's principal interagency mechanism for coordinating the federal effort to respond to and recover from cyber incidents of national significance and includes 19 federal agencies including the Intelligence Community. The NCSD is working with industry to establish a private sector counterpart to the NCRCG, which would communicate and collaborate with the Federal government NCRCG during times of crisis.

Mr. Chairman, further detail regarding the Committee's inquiries related to the goals, resources, and timeframes for implementation associated with these programs is also provided in the Department's recent letter in response to your July 5, 2006 query.

The Role of US-CERT in Internet Recovery

Mr. Chairman, the Committee has expressed concern about the role and responsibility of the United States Computer Emergency Readiness Team with regard to Internet reconstitution.

US-CERT is the operational component of the National Cyber Security Division and represents a partnership between the Department and the public and private sectors. US-CERT is charged with protecting our nation's Internet infrastructure by coordinating defense against and response to cyber attacks. US-CERT is responsible for:

- Analyzing and reducing cyber threats and vulnerabilities;
- Disseminating cyber threat warning information; and
- Coordinating incident response activities.

As indicated above, I am personally overseeing the retooling of the US-CERT and CS&T to ensure that roles and responsibilities align with our mission with regard to Internet recovery and the NRP.

The Role of FEMA in Internet Recovery

Mr. Chairman, the Committee has communicated interest in learning about the role of the Federal Emergency Management Agency (FEMA) with regard to restoration of Internet functions in the case of a major disruption or attack.

Depending upon the nature of the disruption or attack, FEMA, under the direction of the Secretary of Homeland Security, and advised by the Assistant Secretary for Cyber Security and Telecommunications and other Department officials, may be called upon to support industry and other Federal efforts to restore connections to the Internet. FEMA's specific responsibilities under the National Response Plan through Emergency Support Function (ESF) #5 – Emergency Management may entail providing logistical, communications or administrative support as they would for any other emergency or disaster that they do not have the primary lead role. However FEMA would not have the lead role for Internet restoration.

Conclusion

The National Cyber Security Division has established its mission and priority objectives, developed a strategic plan, and undertaken significant steps to implement its strategic plan across the programs outlined here. Our progress to date is tangible: we have a construct for public-private partnership; we have a track record of success in our cyber operations; we have established relationships at various levels to manage cyber incidents; we have built international communities of interest to address a global problem; and we have tested ourselves at a critical development stage and will continue to examine our internal policies, procedures, and communications paths in future exercises. We are building on each of these achievements to take further steps to address Internet recovery and reconstitution as well as to increase our overall cyber preparedness and improve our response and recovery capabilities.

In this ever-evolving environment, we know that we must always be attuned to new threats, new vulnerabilities, and new technologies. We need to be flexible enough to adjust our efforts to meet these new challenges.

I would like to thank the Subcommittee for its time today, and I appreciate this opportunity to bring further transparency to these important cyber security priorities.